CLAIMS

What is claimed is:

1. A computer system comprising:

a central processing unit (CPU);

a chipset, coupled to the CPU, including:

protected registers; and

a host controller;

a bus coupled to the host controller; and

a peripheral device coupled the bus, wherein trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device upon startup of the computer system to verify that the peripheral device is trustworthy.

2. The computer system of claim 1 wherein the encryption data is generated at the peripheral device and transmitted to the host controller.

3. The computer system of claim 1 wherein the encryption data is generated at the CPU and transmitted to the peripheral device.

4. The computer system of claim 1 wherein the trusted software writes to the protected register to indicate to the host controller the encrypted data to transmit and response data that is to be received.

5. The computer system of claim 1 wherein the chipset further comprises:

a protected memory table; and

a memory controller coupled to the memory device.

6. The computer system of claim 5 further comprising a memory device coupled to the memory controller.

7. The computer system of claim 6 wherein the data transmitted between the host controller and the peripheral device bypasses a stack at the memory device associated with the peripheral device.

8. The computer system of claim 7 wherein the memory device comprises:
a protected memory table; and
a trusted software monitor.

9. The computer system of claim 1 wherein the peripheral device is a keyboard.

10. The computer system of claim 1 wherein the peripheral device is a mouse.

11. The computer system of claim 1 wherein the peripheral device is a scanner.

12. The computer system of claim 1 wherein the bus is a Universal Serial Bus.

13. A chipset comprising:
protected registers; and
a host controller coupled to a peripheral device via a bus;
wherein trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device to verify that the peripheral device is trustworthy.

14. The chipset of claim 13 wherein the encryption data is generated at the peripheral device and transmitted to the host controller.

15. The chipset of claim 13 wherein the encryption data is received from a CPU coupled to the chipset and transmitted to the peripheral device.

16. The chipset of claim 13 wherein the trusted software writes to the protected register to indicate to the host controller the encrypted data to transmit and response data that is to be received.

17. The chipset of claim 13 wherein the chipset further comprises:

a protected memory table; and

a memory controller coupled to the memory device.

18. A method comprising:

generating an encryption key within a computer system using trusted software;

the trusted software writing to trusted registers within the computer system to initiate transmission of the encrypted key to a peripheral device; and

transmitting the encryption key to the peripheral device.

19. The method of claim 18 wherein the encryption key is transmitted to the peripheral device while bypassing a memory stack associated with the peripheral device.

20. The method of claim 18 further comprising verifying whether the peripheral device is operating based upon the encryption key.

21. A computer system comprising:

a central processing unit (CPU);

a chipset, coupled to the CPU, including:

protected registers; and

a host controller;

a memory device coupled to the chipset;

a bus coupled to the host controller; and

a peripheral device coupled the bus, wherein trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device upon startup of the computer system to verify that the peripheral device is trustworthy.

22. The computer system of claim 21 wherein the encryption data is generated at the peripheral device and transmitted to the host controller.

23. The computer system of claim 21 wherein the encryption data is generated at the CPU and transmitted to the peripheral device.

24. The computer system of claim 21 wherein the trusted software writes to the protected register to indicate to the host controller the encrypted data to transmit and response data that is to be received.

25. The computer system of claim 21 wherein the chipset further comprises:
a protected memory table; and
a memory controller coupled to the memory device.

26. The computer system of claim 21 wherein the data transmitted between the host controller and the peripheral device bypasses a stack at the memory device associated with the peripheral device.

27. The computer system of claim 21 wherein the memory device comprises:
a protected memory table; and
a trusted software monitor.

28. The computer system of claim 21 wherein the peripheral device is a keyboard.

29. The computer system of claim 21 wherein the peripheral device is a mouse.

30. The computer system of claim 21 wherein the peripheral device is a scanner.

31. The computer system of claim 21 wherein the bus is a Universal Serial Bus.